REMARKS

Claims 1-4 and 6-43 are pending and have been rejected. Claims 1-4 and 7-8 were rejected under 35 U.S.C. § 102(b) as being anticipated by "The Operational Semantics of a Java Secure Processor," by Hartel, *et al.,* dated 1/16/1998 ("Hartel"). Claims 9-11, 13-21, and 33-36 were rejected under 35 U.S.C. § 103(a) as being obvious over Hartel in view of U.S. Patent 6,157,721 to Shear, *et al.* ("Shear"). Finally, claims 6, 12, 22-32 and 37-43 were rejected under 35 U.S.C. § 103(a) as being obvious over Hartel in view of Shear, and further in view of U.S. Patent 5,696,975 to Moore, *et al.* ("Moore").

For at least the reasons set forth below, Applicants respectfully request reconsideration of these rejections.

I. Claims 1-4 and 7-8 Are Not Anticipated By Hartel

The Office Action rejected claims 1-4 and 7-8 as being allegedly anticipated by Hartel. Applicants respectfully disagree. Independent claim 1 recites, among other things, the limitation of determining "whether the applet is ***capable*** of being executed by the secure processor . . . and installing the applet on the secure processor if the secure processor is ***capable*** of executing the applet." (Emphasis supplied). Claims 2-4 and 7-8 depend from claim 1, and thus also include these limitations.

Hartel does not disclose or suggest determining whether an applet is capable of being executed by a secure processor, nor installing the applet if it is in fact so capable, as recited by claims 1-4 and 7-8. Rather, Hartel describes digitally signing applets as a method of detecting tampering, *i.e.,* verifying the integrity of the applet by digital signature. The claim, by contrast, recites determining from at least a portion of the applet whether the applet is ***capable*** of being executed by the secure processor.

Verifying the integrity of an applet, as described by Hartel, is not the same as verifying whether it is capable of being executed by the secure processor, as recited in claims 1-4 and 7-8. Whether or not an applet has been tampered with has no bearing on whether or not the applet is capable of being executed. Further, the act of verifying whether or not an applet has been tampered with is different from the act of determining whether an applet is capable of being executed.

Moreover, the specification of the present application clearly distinguishes between using digital signatures to verify that data has not been tampered with, and what claims 1-4 and 7-8 recite, which is determining whether an applet is capable of being executed by the secure processor. For example, paragraph [0033] of the specification, in describing Fig. 4, states that at step 406 "secure processor 180 verifies the data integrity of the security meta-data portion 212 and the resource meta-data portion 214 against the meta-data signature portion 216 using a public key verification algorithm." In a separate step 408, paragraph [0034] of the specification describes one non-limiting example of how the claimed step of determining whether the applet is capable of being executed by the secure processor would be performed:

> The availability of the necessary resources on the secure processor 180 is verified at step 408. The resource meta-data portion 214 specifies a number of resources the executable may need when executed. Preferably, the resource meta-data portion 214 specifies every resource the executable may need when executed. All the resources specified in the resource meta-data portion 214 must be available on the secure processor 180 in order to install the applet 200. The resources may be currently used by another process when the applet 200 is installed, but at execution, all the specified resources must be at the disposal of the applet 200. If the secure processor 180 has the necessary resources, the temporary variable resource is set to TRUE to designate that the required resources are present in the secure processor 180.

Specification at [0034].

In short, verifying data integrity, *i.e.*, that data has not been tampered with, is not the same as determining whether an applet is capable of being executed by the secure processor. Since Hartel describes only the verification of data integrity, and does not disclose or suggest the claimed limitation of determining whether an applet is capable of being executed by the secure processor, Hartel does not anticipate claims 1-4 and 7-8. Withdrawal of the rejection of claims 1-4 and 7-8 as anticipated by Hartel is respectfully requested.

II. Claims 9-11, 13-21, and 33-36 Are Not Obvious Over the Combination of Hartel and Shear

Claims 9-11 and 13-21 also depend from claim 1, and thus also recite the limitation of "with the secure processor, determining from at least a portion of the applet whether the applet is ***capable*** of being executed by the secure processor . . . and installing the applet on the secure processor if the secure processor is ***capable*** of executing the applet." (Emphasis supplied). Claims 33-36 include these limitations as well.

As was explained in the previous section, Hartel fails to disclose or suggest this limitation, and is thus defective as an anticipatory reference against claims 9-11, 13-21, and 33-36. Moreover, the Office Action does not cite to any portion of Shear that would cure this defect in Hartel, nor was Shear cited for this purpose. Thus, it is submitted that the combination of Hartel and Shear fails to render claims 9-11, 13-21, and 33-36 obvious. Applicants respectfully request withdrawal of this rejection as well.

III. Claims 6, 12, 22-32 and 37-43 Are Not Obvious Over the Combination of Hartel, Shear and Moore

Claims 6, 12, and 22-29, and 37 also recite the limitation of determining "whether the applet is ***capable*** of being executed by the secure processor . . . and installing the applet on the secure processor if the secure processor is ***capable*** of executing the applet." (Emphasis supplied). As was previously explained in connection with Applicants' response to the rejection of claims 9-11 and 13-21, and 33-36, the combination of Hartel and Shear fails to disclose or suggest this limitation, and in thus defective as a basis for rejecting as obvious claims 6, 12, and 22-29. Moore does not cure this defect in the combination of Hartel and Shear, nor was Moore cited in the Office Action for this purpose. Thus, it is submitted that the combination of Hartel and Shear with Moore fails to render claims 6, 12, and 22-29 obvious, and Applicants respectfully request withdrawal of this rejection as well.

As for claims 30-32, each of these includes the limitations of

receiving a request from a secure processor for a list of alternative applets;
the request comprising:
an applet serial number which identifies a first applet;
an identifier which identifies the secure processor;
a first indicator which identifies a security rating of the secure processor; and
a second indicator which identifies the at least one resource of the computer;
creating the list of alternative applets from the plurality of applets based at least in part on the first indicator and the second indicator; and
transmitting the list of alternative applets to the computer.

The Office Action cites to no portion of either Hartel, Shear or Moore that discloses or suggests creating a list of alternative applets based at least in part on a first indicator that identifies a security rating and a second indicator that identifies at least one

resource of the computer, as recited by claims 30-32, nor does such a portion exist. As such, there is no combination of Hartel, Shear and/or Moore that renders claims 30-32 obvious, and Applicants respectfully request that the rejection of these claims be withdrawn.

Finally, as to claims 38-43, each of those claims recites a secure applet comprising

> a meta-data portion, said meta-data portion including:
> a security meta-data portion;
> a resource meta-data portion; and
> a meta-data signature portion;
> an executable portion, said encrypted executable portion including:
> an encrypted executable portion; and
> an unencrypted executable signature portion; and
> a certificate portion.

Again, the Office Action cites to no portion of either Hartel, Shear or Moore that discloses a secure applet comprising each of the elements recited in claims 38-43. Rather, the Office Action merely asserts in conclusory fashion:

> As per claims 37-40, this is a system version of the claimed method discussed above in claims 1, 2, 8-16, 20, 22 and 24, wherein all claimed limitations have also been addressed and/or cited as set forth above. For example, see the Hartel/Shear/Moore system, (Hartel p. 1:20-6:40, Shear col. 5:1-5 and 22:27-40 and Moore col. 1:29-8:20).

Office Action at p. 15.

Applicants respectfully disagree. None of the cited portions of Hartel, Shear or Moore, nor any other portion of those references for that matter, disclose or suggest the elements of a secure applet recited by claims 38-43. As such, the rejection of claims 38-43 as obvious over the combination of Hartel, Shear and Moor is improper and should be withdrawn.

IV. Conclusion

Applicants respectfully request that the Examiner consider the above remarks and allow the claims to issue.

Respectfully submitted,

Gary M. Butter
Reg. No. 33,841
Attorney for Applicants

BAKER BOTTS L.L.P.
Customer No. 21003
30 Rockefeller Plaza
New York, NY 10112
(212) 408-2628